COLORADOGOP

FOR IMMEDIATE RELEASE

COLORADO ELECTION PASSWORDS LEAKED AND SYSTEM MAY BE COMPROMISED

(Greenwood Village, CO) – According to an affidavit sent to the Republican Party of Colorado, Colorado Secretary of State, Jena Griswold, shared a file on her website that contained over 600 BIOS passwords for voting system components in 63 of the state's 64 counties. On Thursday, October 24, 2024, those BIOS passwords were discretely removed by an unnamed official. A letter from the Colorado GOP has been sent to the Colorado Secretary of State's Office and can be reviewed below.

The passwords were not encrypted or otherwise protected – this means they were available for public consumption. The file appears to have been posted at least since August; the amended version[1] of the file was reposted last Thursday.

BIOS passwords are highly confidential, allowing broad access for knowledgeable users to fundamentally manipulate systems and data and to remove any trace of doing so. Due to the sensitivity surrounding BIOS passwords, Colorado election regulation (8 CCR 1505-1), Rule 20.5.2(c)(11), requires limited access to a select few at the Colorado Department of State; neither county clerks nor commissioners have access to these files.

While the above does not constitute evidence of a breach by itself, it

does demonstrate a major lapse in basic systems security and password management.

"We hear all the time in Colorado from Secretary Griswold and Governor Polis that we represent the 'Gold Standard' for election integrity, a model for the nation," said **Dave Williams, Chairman of the Republican Party of Colorado**. *"One can only hope that by the Secretary of State posting our most sensitive passwords online to the world dispels that myth." said Williams.*

A bad actor would still need access either physically or remotely to the systems.[2] It is also unclear whether the passwords were in use at any point while publicly available.

"It's shocking really. At best, even if the passwords were outdated, it represents significant incompetence and negligence, and it raises huge questions about password management and other basic security protocols at the highest levels within Griswold's office," said Williams. This type of security breach could have far-reaching implications, putting the entire Colorado election results for the vast majority of races, including the tabulation for the Presidential race in Colorado, in jeopardy unless all of the machines can meet the standards of a "Trusted Build" before next Tuesday.

Vote tabulation in Colorado using the voter systems is already underway with results intended to be inaccessible until the close of polls next week.

###

---

[1] Link: "Voter System Inventory – 2024 (XLSX)": https://www.sos.state.co.us/pubs/elections/VotingSystems/VSHomePage1.html

[2] Heidi Ganahl, the Republican candidate for governor in 2022, recently highlighted concerns regarding remote access to Colorado voting systems. See: https://youtu.be/RgG-ysUlvq4?si=QDJUTuQaDKSxDmvh

October 29, 2024

The Honorable Jena Griswold
Colorado Secretary of State
1700 Broadway
Suite 200
Denver, CO 80290-1201

Re: Your Public Disclosure of the BIOS Passwords for Colorado Election Systems Dear Secretary Griswold:

It has come to our attention this week that last Thursday, October 24, 2024, your team quietly removed a publicly accessible spreadsheet file from the Colorado Secretary of State's website that contained BIOS passwords for election systems in 63 of the 64 counties in Colorado.

The passwords were not encrypted or otherwise protected. They were open to the public for anyone with the knowledge or wherewithal to look (located simply on hidden sheets within the spreadsheet, a file that appears to have been posted publicly for months).

As you are well aware, a BIOS password could allow a knowledgeable user to not only gain total control over any system accessed either physically or remotely, including the ability to manipulate those systems and results, but it would allow that user to remove any trace that she was ever there (overwriting even fundamental system logs necessary during a subsequent audit to show whether illicit access or activity had ever occurred).

It goes without saying how significant this is. We realize that a bad actor or actors would still need access to the systems, but this, coupled with the recent discoveries about network access announced by Heidi Ganahl, former Republican Candidate for Governor, just weeks ago, should give every party, every candidate, and every voter serious concerns.

We can only imagine that, since the discovery last week, you and your

staff have been working tirelessly to remedy these vulnerabilities. To ensure us and the public that the election in a little over a week is indeed secure, we demand you provide the following in writing:

- Confirmation that all passwords disclosed have since been changed or were otherwise not current at any point while made public;
- Confirmation that all new passwords, their storage, and management meet best practices for password strength and encryption, unlike those publicly disclosed;
- Confirmation that all systems are running the current software as necessary for proper certification, as the hidden pages also provided software certification concerns;
- If the passwords were current at any point while public, confirmation that, to the best of your knowledge, the election systems have not been accessed physically or remotely by any unauthorized person or persons, including any individuals otherwise authorized to access the systems but not the system BIOS;
- Understanding that with BIOS access it may be difficult or impossible to identify if a system has been indeed compromised, provide confirmation or a detailed plan as to how all exposed systems still or will meet the certification requirements of a "trusted build" before any votes are counted by those systems in this election; and
- Provide a list of any and all other steps your team has or is taking to address these vulnerabilities, including when any steps still pending will be completed.

While some may attempt to characterize this letter as a fringe or partisan issue, we are confident that you understand the critical nature of having released these "skeleton key" passwords to the world. As such, we fully expect that you will gladly and forthrightly provide us with all that we are asking, using the same standard and diligence you are applying in Mesa County and understanding that best practices would be for you to already have those steps completed or in process. If, however, you fail to provide necessary assurances that our elections are secure, we are prepared to encourage county officials throughout the state to fulfill their duty to decertify any election machines with a password on the released list and to compel you through C.R.S. 1-1-113 to secure the elections, as required by law.

required by law.

Given that the election is now in a matter of days, kindly provide your response within twenty- four hours.

Sincerely,

Dave Williams
Chairman, Republican Party of Colorado

CC: The Honorable Merrick Garland, United States Attorney General
The Honorable Matt Kirsch, Acting United States Attorney for the District of Colorado
The Honorable Sean Cooksey, Chairman of the Federal Election Commission
The Honorable Jared Polis, Governor of Colorado
The Honorable Phil Weiser, Colorado Attorney General
Boards of County Commissioners for Colorado
Colorado County Clerks and Recorders
CO Political Party Chairs

AFFIDAVIT

STATE OF COLORADO)
)
COUNTY OF [redacted])

I, [redacted], declare under oath that the following facts are true:

1. I am over the age of eighteen years, competent in all respects to make this affidavit, and I have personal knowledge of the matters set forth herein.
2. On three occasions in 2024 (8 August 2024, 16 October 2024, and 23 October 2024), I

have accessed through the Internet the Colorado Secretary of State website (www.coloradosos.gov) and "Voting Systems" webpage[1] and have used a link which is no longer available on that page, but which was previously available through at least 23 October 2024[2] to download a 562 KB Microsoft Excel file named "VotingSystemInventory.xlsx."

3. That VotingSystemInventory.xlsx file, upon downloading and opening with the Microsoft Excel application, contains one visible worksheet named "Inventory," listing voting system components by county, showing one row for each component and columns titled "Serial #," "County," "Model," "Vendor," "Remarks," "Inactive," and "Firmware/Software Version."

4. The same VotingSystemInventory.xlsx file, upon right-clicking the Worksheet Tab section of the main screen and selecting "Unhide," opens a dialog box where the application user can select from one, several, or all four listed hidden worksheets contained in the file. The four hidden worksheets are named "Clean_Formulas," "OLD_EquipmentDatabase," "OLD_working," and "OLD_ICXs."

5. Upon unhiding and viewing those previously hidden worksheets, three of the four worksheets (all but "OLD_ICXs") appear to list Basic Input Output System (BIOS) passwords for some listed components.[3] In the worksheets "Clean_Formulas" and

---

[1] https://www.coloradosos.gov/pubs/elections/VotingSystems/VSHomePage1.html
[2] https://web.archive.org/web/20240719205353/https://www.coloradosos.gov/pubs/elections/VotingSystems/VSHomePage1.html
[3] Components for which BIOS passwords appear to be listed/associated, include Dominion Voting System (DVS) Democracy Suite voting system: Election Management System (EMS) Standard Servers and Express Servers, EMS Client workstations, Adjudication Client workstations, ImageCast Central (ICC) scanner/tabulators; and ClearBallot Group (CBG) ClearVote voting system DesignStations, Administration Stations, DesignServers, and ScanServers.

"OLD_EquipmentDatabase," those passwords are shown in a column titled "BIOS Password," and those passwords can, again, be associated with specific components in specific counties by the data for each row in columns titled "Serial #," "County," "Model," "Vendor," and "Device Type."

6. The "Clean_Formulas" worksheet lists BIOS passwords for over 700 individual voting system components in 63 Colorado counties' voting systems; the only county for which no voting system component BIOS password is listed is Las Animas County.

7. Comparison of values in the "Serial #" columns of the "Inventory" and "Clean_Formulas" worksheets indicates that the "Clean_Formulas" worksheet lists BIOS passwords for voting system components that are currently in use in at least ten of Colorado's twelve largest

counties, by population. [redacted]

Subscribed and sworn to before me this 27th day of October, 2024, by [redacted].

[redacted]
NOTARY PUBLIC
STATE OF COLORADO
[redacted]
MY COMMISSION EXPIRES [redacted]

[redacted]

Notary Seal

Paid for by Colorado Republican Committee. Not authorized by any candidate or candidate's committee. www.cologop.org

cologop.org

Colorado Republican State Party
5950 S. Willow Drive, Suite 210

Greenwood Village, Colorado 80111

This message reflects the opinions and representations of the Colorado Republican Party. You are receiving this email because you signed up as a member of the Colorado Republican Party's online community. If you would prefer not to receive future emails from the Colorado GOP, click here.

Copyright © 2022 - Colorado Republican Party
All rights reserved.

You can update your preferences or unsubscribe from this list